# Affirmative Evidence

## Affirmative Definitions

### Digital Surveillance

#### Digital Surveillance involves monitoring data and traffic on the internet

Nikki Gulzar, Basra Abbasi, Eddie Wu, Anil Ozbal, & WeiQi Yan, 2013 [Auckland University of Technology], “Surveillance Privacy Protection” http://staff.elena.aut.ac.nz/Wei-Yan/VC/articles/SPP.pdf

One of the cutting-edge surveillance technologies is digital surveillance. It involves the monitoring data and traffic on internet [64]. Government agencies such as Information Awareness Office, NSA and the FBI spend billions of dollars each year to develop systems so as to intercept and analyze the data transmitted, and extract the data that is useful to law enforcements [14].

### Privacy

#### The Right to Privacy is narrowly defined

Cornell University Law School, Copyright 2014 “Right to Privacy: An Overview” <http://www.law.cornell.edu/wex/privacy>

Distinct from the right of publicity protected by state common or statutory law, a broader right of privacy has been inferred in the Constitution. Although not explicity stated in the text of the Constitution, in 1890 then to be Justice Louis Brandeis extolled 'a right to be left alone.' This right has developed into a liberty of personal autonomy protected by the 14th amendment. The 1st, 4th, and 5th Amendments also provide some protection of privacy, although in all cases the right is narrowly defined. The Constitutional right of privacy has developed alongside a statutory right of privacy which limits access to personal information. The Federal Trade Commission overwhelmingly enforces this statutory right of privacy, and the rise of privacy policies and privacy statements are evidence of its work. In all of its forms, however, the right of privacy must be balanced against the state's compelling interests. Such compelling interests include the promotion of public morality, protection of the individual's psychological health, and improving the quality of life. These distinct rights of privacy are examined separately on the following pages:

### National Security

#### National Security is a corporate term that refers to protecting a nation from danger

US Legal, Copyright 2014 “National Security Law & Legal Definition” http://definitions.uslegal.com/n/national-security/

National security is a corporate term covering both national defense and foreign relations of the U.S. It refers to the protection of a nation from attack or other danger by holding adequate armed forces and guarding state secrets. The term national security encompasses within it economic security, monetary security, energy security, environmental security, military security, political security and security of energy and natural resources. Specifically, national security means a circumstance that exists as a result of a military or defense advantage over any foreign nation or group of nations, or a friendly foreign relations position, or a defense position capable of successfully protesting hostile or destructive action.

## Civil Liberties, Privacy, & Constitutional Rights

#### National Security Agency Surveillance is Legal

Bucci, Steven. [Dr., Director of The Heritage Foundation's Douglas & Sarah Allison Center for Foreign Policy Studies]. "Phone Records and the NSA: Legal and Keeping America Safe," Heritage Foundation. June 20, 2013, <http://blog.heritage.org/2013/06/20/phone-records-and-the-> nsa-legal-and-keeping-america-safe/

Over the past week, Snowden has inundated the world with details about the NSA collection of telephone records from companies such as Verizon. However, according to a FISA court order, Verizon was only ordered to hand over “metadata” of the calls it processed. Metadata refers to basic information, including telephone number, location, and duration of the call, and the court order does not authorize the government to access the content of such conversations. There is a growing body of legal precedent for the NSA program. In 1976 the Supreme Court upheld “the third party doctrine,” which states that anyone who voluntarily provides information to a third party, such as a telephone service provider, cannot object if it is later turned over to the government. What’s more, in 1979, the Supreme Court held in Smith v. Maryland that the government did not need a warrant to obtain phone record information as it did for the content of such communications. The information was not constitutionally protected because there was no true expectation of privacy. As a result, metadata collection is not protected under the 4th Amendment and is perfectly legal.

#### Loss of Privacy is Inevitable, Benefits of Surveillance Outweigh the Cost

Rosenzweig, Paul. [Visiting Fellow at Heritage Foundation]. "The State of Privacy and Security - Our Antique Privacy Rules," The Heritage Foundation. August 1, 2012,<http://www.heritage.org/research/testimony/2012/08/the-state-of-privacy-and-security-our-> antique-privacy-rules

Ten years ago, surveying the technology of the time which, by and large, was one hundred times less powerful than today’s data processing capacity Scott McNealy, then-CEO of Sun Microsystems, said, “Privacy is dead. Get over it.”[14] He was, it seems, slightly wrong. Pure privacy—that is, the privacy of activities in your own home—remains reasonably well- protected.[15] What has been lost, and will become even more so increasingly, is the anonymity of being able to act in public (whether physically or in cyberspace) without anyone having the technological capacity to permanently record and retain data about your activity for later analysis. Today, large data collection and aggregation companies, such as Experian and Axicom, may hire retirees to harvest, by hand, public records from government databases.[16] Paper records are digitized and electronic records are downloaded. These data aggregation companies typically hold birth records, credit and conviction records, real estate transactions and liens, bridal registries, and even kennel club records. One company, Acxiom, estimates that it holds on average approximately 1,500 pieces of data on each adult American.[17] Since most, though not all, of these records are governmental in origin, the government has equivalent access to the data, and what they cannot create themselves they can likely buy or demand from the private sector. The day is now here when anyone with enough data and sufficient computing power can develop a detailed picture of any identifiable individual. That picture might tell your food preferences or your underwear size. It might tell something about your terrorist activity. Or your politics. This analytical capacity can have a powerful influence in law and policy and in particular in revealing links between the cyber personas and the real world activities of individuals. When we speak of the new form of “dataveillance,” we are not speaking of the comparatively simple matching algorithms that cross check when a person’s name is submitted for review when, for example, they apply for a job. Even that exercise is a challenge for any government, as the failure to list Abdulmutallab in advance of the 2009 Christmas bombing attempt demonstrates.[18] The process contains uncertainties of data accuracy and fidelity, analysis and registration, transmission and propagation, and review, correction, and revision. Yet, even with those complexities, the process uses relatively simple technologically—the implementation is what poses a challenge.

#### Ending NSA surveillance would equal a disarmament in the war on terror, which is far from over

Boot, Max. [Senior Fellow in National Security Studies at the Council on Foreign Relations]. "Stay calm and let the NSA carry on," The LA Times. June 9, 2013,<http://articles.latimes.com/2013/jun/09/opinion/la-oe-boot-nsa-surveillance-20130609>

Granted there is something inherently creepy about Uncle Sam scooping up so much information about us. But Google, Facebook, Amazon, Twitter, Citibank and other companies know at least as much about us, because they use very similar data-mining programs to track our online movements. They gather that information in order to sell us products, and no one seems to be overly alarmed. The NSA is gathering that information to keep us safe from terrorist attackers. Yet somehow its actions have become a "scandal," to use a term now loosely being tossed around.

The real scandal here is that the Guardian and Washington Post are compromising our national security by telling our enemies about our intelligence-gathering capabilities. Their news stories reveal, for example, that only nine Internet companies share information with the NSA. This is a virtual invitation to terrorists to use other Internet outlets for searches, email, apps and all the rest. No intelligence effort can ever keep us 100% safe, but to stop or scale back the NSA's special intelligence efforts would amount to unilateral disarmament in a war against terrorism that is far from over.

#### Privacy Concerns are NOT Justified

Posner, Eric. [Law professor at the University of Chicago]. "I Don’t See a Problem Here," The New York Times. June 9, 2013, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-> surveillance-threat-real-or-imagined

The first objection strikes me as weak. We already give the government an enormous amount of information about our lives, and seem to have gotten used to the idea that an Internal Revenue Service knows our finances, or that an employee of a government hospital knows our medical history, or that social workers (if we are on welfare) know our relationships with family members, or that public school teachers know about our children’s abilities and personalities. The information vacuumed up by the N.S.A. was already available to faceless bureaucrats in phone and Internet companies — not government employees, but strangers just the same. Many people write as though we make some great sacrifice by disclosing private information to others, but it is in fact simply the way that we obtain services we want — whether the market services of doctors, insurance companies, Internet service providers, employers, therapists and the rest, or the nonmarket services of the government like welfare and security. Even so, I am exaggerating the nature of the intrusion. The chance that human beings in government will actually read our e- mails or check our phone records is infinitesimal (though I can understand that organizations like the A.C.L.U. that have a legitimate interest in communicating with potential government targets may be more vulnerable than the rest of us). Mostly all we are doing is making our information available to a computer algorithm, which is unlikely to laugh at our infirmities or gossip about our relationships.

#### NSA Surveillance Protects Against Terror Attacks

Nye, Joseph. [Professor of Government at Harvard University]. "Privacy gains the upper hand in the NSA surveillance debate," The Daily Star. August 19, 2013, <http://www.dailystar.com.lb/Opinion/Commentary/2013/Aug-19/227751-privacy-gains-the-upper-> hand-in-the-nsa-surveillance-debate.ashx#axzz2hEwSq0Dd

Rather than demonstrating hypocrisy and acceptance of the erosion of civil liberties, the Snowden disclosures have provoked a debate that suggests the U.S. is living up to its democratic principles in its traditionally untidy ways. America faces a trade-off between security and liberty, but the relationship is more complex than it appears at first glance. The worst threats to liberties come when insecurity is greatest, so modest trade-offs can sometimes prevent greater losses. Even such a great defender of freedom as Abraham Lincoln suspended habeas corpus under the extreme conditions of the American Civil War. And such decisions may not be recognized as mistaken or unjust until later – consider Franklin Roosevelt’s internment of Japanese-American citizens early in World War II. In the decade after Sept. 11, 2001, the pendulum of public sentiment swung too far to the security pole; but it has begun to swing back in the absence of major new terrorist attacks. A recent ABC News-Washington Post poll showed that 39 percent of Americans now say that protecting privacy is more important than investigating terrorist threats, up from only 18 percent in 2002. Ironically, the programs that Snowden revealed seem to have helped prevent massive new terrorism events, such as a bomb attack on the New York subways. If so, they may have prevented the implementation of more draconian anti-terrorist measures – thus enabling the current debate.

#### Civil Liberties are Well Protected

Gerecht, Reuel. [senior fellow at the Foundation for Defense of Democracies and a former case officer in the CIA’s clandestine service]. "The Costs and Benefits of the NSA," The Weekly Standard. June 24, 2013, [http://www.weeklystandard.com/articles/costs-and-benefits- nsa\_735246.html](http://www.weeklystandard.com/articles/costs-and-benefits-%20nsa_735246.html)

But journalists in Washington, who rub shoulders every day with national-security types, surely know that America isn’t that far gone. Civil liberties after 12 years of the global war on terrorism are actually as strongly protected in America as they were in 1999, when Bill Clinton was treating terrorism as crime and his minions were debating the morality of assassinating Osama bin Laden. The same is true in France and Great Britain, liberal democracies that have the finest, but also the most intrusive, counterterrorism forces in the West. Surveillance in these countries is intimate—the French internal-security service, the DST, and British domestic intelligence, MI5, bug and monitor their countrymen in ways that remain unthinkable in the United States. Yet the political elites and the societies of both countries have become much more sensitive to, and protective of, personal freedom as their internal security forces have grown more aggressive. It’s an odd and, for those attached to Friedrich Hayek’s Road to Serfdom, disconcerting development: The massive American government, born of the welfare state and war, hasn’t yet gone down the slippery fascist slope. Liberal welfare imperatives may be bankrupting the country, but they have not produced a decline of most (noneconomic) civil liberties. Just the opposite. American liberalism’s focus on individual privacy and choice has, so far, effectively checked the creed’s collectivism. America’s national-security state, which Greenwald believes has already become a leviathan, is, for the most part, rather pathetic.

## Cybersecurity

#### US Cyber Infrastructure is at High Risk

Andrea Seabrook [NPR Staff Reporter] “It’s the next war: Protecting the nation’s critical infrastructure from cyber attack” July 3, 2014 <http://www.wptv.com/decodedc/podcast/its-the-next-war-protecting-the-nations-critical-infrastructure-from-cyber-attack>

In the age of cyber warfare, security takes on new meaning. You may worry about your email or credit cards getting hacked. But government computer security experts warn of a different, and potentially much more dangerous risk – a cyber attack on the nation’s critical infrastructure. That means power plants, oil pipelines, drinking water supplies, major ports of commerce -- anything that American communities rely on to keep society running smoothly.

This critical infrastructure is increasingly operated by computers and special software called Industrial Control Systems. That means greater efficiency and much more convenience for many people. Advances in the so called “smart electricity grid” alone could save money and fossil fuels, as well as send more power to the parts of the grid that need it when they need it.

But those sophisticated Industrial Control Systems are exactly what make the United State more vulnerable, say auditors at the Government Accountability Office.

#### Current Legislation Hinders NSA Efforts to Thwart Cyberattacks

Brendan Sasso [Technology Policy Analyst] “Senate Panel Passes Cybersecurity Bill Despite NSA Fears” July 8, 2014 http://www.nationaljournal.com/tech/senate-panel-passes-cybersecurity-bill-despite-nsa-fears-20140708

The Cybersecurity Information Sharing Act, advanced in a 12-3 vote, would make it easier for businesses and the government to share information with each other about cyberattacks. Business groups argue that legal barriers are preventing them from getting the information they need to stop hackers.

"Every week, we hear about the theft of personal information from retailers and trade secrets from innovative businesses, as well as ongoing efforts by foreign nations to hack government networks," Senate Intelligence Committee Chairwoman Dianne Feinstein said in a statement. "This bill is an important step toward curbing these dangerous cyberattacks."

The legislation includes provisions aimed at protecting privacy, such as requiring that companies that share information first strip out personally identifiable data (such as names, addresses, and Social Security numbers) of known Americans.

But the privacy groups are still worried that the legislation could encourage a company such as Google to turn over vast batches of emails or other private data to the government. The information would go first to the Homeland Security Department, but could then be shared with the NSA or other intelligence agencies.

"Instead of reining in NSA surveillance, the bill would facilitate a vast flow of private communications data to the NSA," the American Civil Liberties Union, the Center for Democracy and Technology, the Electronic Frontier Foundation, and dozens of other privacy groups wrote in a letter to senators last month.

Democratic Sens. Ron Wyden and Mark Udall voted against the legislation, saying in a statement that it "lacks adequate protections for the privacy rights of law-abiding Americans, and that it will not materially improve cybersecurity."

The senators said they don't trust the government not to exploit loopholes to spy on Americans. According to a Wyden aide, the committee defeated an amendment that the Oregon Democrat offered that would have strengthened privacy protections.

The legislation is a counterpart to the Cyber Intelligence Sharing and Protection Act, which passed the House last year.

That legislation prompted a major backlash from Internet activists, who fear it would undermine Internet privacy. More than 100,000 people signed a White House petition opposing the bill, and "CISPA" became a dirty word on many blogs, discussion forums, and news sites.

The White House issued a veto threat on CISPA, saying it lacked adequate privacy safeguards.

"I don't know what information you would be concerned about that NSA would have in an information-sharing bill," Feinstein told reporters following the markup, which was closed to the public. "If somebody's hacking, you want [the information] to go where it needs to go."

She said the legislation is just a "first step" in improving cybersecurity, and that she is hopeful it will become law before the end of the year.

Sen. Saxby Chambliss, the committee's top Republican, said the bill is a carefully crafted compromise between business groups and privacy advocates.

"It's not perfect for anybody," Chambliss told reporters. "But if we take no action, then cyberattacks are going to continue to occur, and there is the potential for the American economy to be severely disrupted."

## Binary Searches

#### Binary Searches Limit Privacy Invasion

Ric Simmons, [Professor of Law, Ohio State University], "Ending the Zero-Sum Game: How to Increase the Productivity of the Fourth Amendment," Harvard Journal of Law & Public Policy, 2012.

Binary surveillance refers to a surveillance method that only produces one of two results: positive (meaning that illegal activity has been detected) or negative (meaning that illegal activity has not been detected).92 The surveillance provides no other information about the person or area being monitored, and so represents a relatively minor intrusion on the target’s privacy. In fact, the Supreme Court has held that binary surveillance does not even count as a “search” under the Fourth Amendment because it does not infringe on an expectation of privacy that society is prepared to recognize as legitimate.93 A simple example of a binary surveillance technique is a field test for narcotics. If a law enforcement officer reasonably believes that a certain substance may be narcotics, she can legally seize a very small amount of the substance and mix it with certain chemicals.94 If the substance tests positive for narcotics, the law enforcement officer knows that the substance is in fact contraband and that a crime has occurred. If the substance tests negative, the officer knows nothing about the substance other than the fact that it is not an illegal drug. Therefore, because the suspect has no legitimate interest in possessing contraband, assuming other procedural prerequisites are satisfied, the surveillance does not implicate the Fourth Amendment95—the officer either learns nothing at all about the defendant or learns that the defendant is engaging in illegal activity.

## Democracy

#### Surveillance Helps, not Hinders, Democracy

Posner, Eric. [Law professor at the University of Chicago]. "The Secrecy Paradox," The New York Times. June 9, 2013, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-> threat-real-or-imagined

This brings me to another valuable point you made, which is that when people believe that the government exercises surveillance, they become reluctant to exercise democratic freedoms. This is a textbook objection to surveillance, I agree, but it also is another objection that I would place under “theoretical” rather than real. Is there any evidence that over the last 12 years, during the flowering of the so-called surveillance state, Americans have become less politically active? More worried about government suppression of dissent? Less willing to listen to opposing voices? All the evidence points in the opposite direction. Views from the extreme ends of the political spectrum are far more accessible today than they were in the past. It is infinitely easier to get the Al Qaeda perspective today — one just does a Google search — than it was to learn the Soviet perspective 40 years ago, which would have required one to travel to one of the very small number of communist bookstores around the country. It is hard to think of another period so full of robust political debate since the late 1960s — another era of government surveillance.

## Governmental Secrecy

#### Secret Government Programs are Necessary and Effective

Posner, Eric. [Law professor at the University of Chicago]. "The Secrecy Paradox," The New York Times. June 9, 2013, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-> threat-real-or-imagined

The question raises a real paradox. If government can keep secrets, then the public cannot hold it to account for its actions. But if government cannot keep secrets, then many programs — including highly desirable ones — are impossible. Many commentators seem to think that the answer is to keep secrecy to an absolute minimum, but this response is far too easy. One reason it is too easy is that it implies that secrecy can be exceptional. Government secrecy in fact is ubiquitous in a range of uncontroversial settings. To do its job and protect the public, the government must promise secrecy to a vast range of people — taxpayers, inventors, whistle- blowers, informers, hospital patients, foreign diplomats, entrepreneurs, contractors, data suppliers and many others. But that means that the basis of government action, which relies on information from these people, must be kept secret from the public. Economic policy is thought to be open, but we saw during the financial crisis that government officials needed to deceive the public about the health of the financial system to prevent self-fulfilling runs on banks. Then there are countless programs that are not secret but that are too complicated and numerous for the public to pay attention to — from E.P.A. regulation to quantitative easing. N.S.A. surveillance blends into this incessant, largely invisible background buzz of government activity; there is nothing exceptional about it.

## Surveillance is Vital

#### Surveillance is key to national security

Alan Dershowitz, [Harvard University], Debate with Michael Hayden, Alexis Ohanian, and Glenn Greenwald, Toronto, transcript available at The Atlantic, http://www.theatlantic.com/politics/archive/2014/05/false-equivalence-on-surveillance-from-alan- dershowitz/361694/, May 5, 2014.

Our enemies, especially those who target civilians, have one major advantage over us. They are not constrained by morality or legality. We have an advantage over them. In addition to operating under the rule of law, we have developed through hard work and extensive research technological tools that allow us to monitor and prevent their unlawful and lethal actions. Such technological tools helped us break the German and the Japanese code during the Second World War. They helped us defeat fascism. They helped us in the Cold War. And they are helping us now in the hot war against terrorists who would bomb this theater if they had the capacity to do so. You're going to hear again that there are only excuses that are being offered, that terrorism is really not a serious problem, or that American policy is as terroristic as the policy of al-Qaeda. I don't think you're going to accept that argument.

#### Balanced Constraints on Surveillance Helps Preserve National Security

Alan Dershowitz, [Harvard University], Debate with Michael Hayden, Alexis Ohanian, and Glenn Greenwald, Toronto, transcript available at The Atlantic, http://www.theatlantic.com/politics/archive/2014/05/false-equivalence-on-surveillance-from-alan- dershowitz/361694/, May 5, 2014.

We need to know what harms our enemies, external and internal, are planning in order to prevent them from carrying them out. We also need to impose constraints. And that's why process comes into play. We need a demanding process. But we need to make sure that the burden is realistically designed to strike a proper balance between two equally legitimate but competing values, the need for intelligence to stop attacks against us and the need to protect our privacy from those who place too high a value on security and too low a value on privacy. I believe it is possible to strike that balance in a manner that protects our freedoms, and that is where our efforts should be directed. Surveillance properly limited and appropriately conducted can promote liberty, protect life, and help us defend our freedoms.

## Terrorism

#### NSA Surveillance Has Thwarted Terrorist Plots

Kimberly Dozier, [Associated Press], "NSA: Surveillance Programs Foiled Some 50 Terrorist Plots Worldwide," Huffington Post, June 18, 2013.

Intelligence officials have disclosed some details on two thwarted attacks, and Alexander promised additional information to the panel on thwarted attacks that the programs helped stop. He provided few additional details. The programs "assist the intelligence community to connect the dots," Alexander told the committee in a rare, open Capitol Hill hearing. Alexander got no disagreement from the leaders of the panel, who have been outspoken in backing the programs since Edward Snowden, a 29-year-old former contractor with Booz Allen Hamilton, disclosed information to The Washington Post and the Guardian newspapers.

#### NSA Surveillance Continues to Prevent Terrorism and Efforts should be Increased

Bucci, Steven. [Dr., Director of The Heritage Foundation's Douglas & Sarah Allison Center for Foreign Policy Studies]. "Phone Records and the NSA: Legal and Keeping America Safe," Heritage Foundation. June 20, 2013, <http://blog.heritage.org/2013/06/20/phone-records-and-the-> nsa-legal-and-keeping-america-safe/

U.S. law enforcement and Intelligence agencies depend on tools and methods, such as the leaked NSA program, to combat homegrown radicalization and to fight the ongoing threat from terrorist cells such as the Al-Qaeda in the Arabian Peninsula in Yemen. Moreover, NSA Director General Keith Alexander testified to Congress that these surveillance programs have helped foil dozens of terrorist attacks. These include, he stated, an attempted suicide plot against the New York City subway system by Najibullah Zazi, who pleaded guilty. Since 9/11, the U.S. has thwarted over 50 terrorist plots against America’s homeland. In addition to continued reliance on counterterrorism devices such as the Patriot Act and the NSA surveillance programs, Congress must take action to plug the remaining gaps in our counterterrorism system. For instance, there should be increased visa coordination to prevent known terrorists from boarding airplanes and travelling to the U.S. Additionally, Congress should foster greater cooperation among local, state, and federal agencies to streamline their information-sharing capabilities. The current debate raging over Snowden’s leaking of the secret NSA surveillance program is no doubt a healthy exercise for a thriving democracy. The scope of the metadata collection and how the government uses it should come under close scrutiny. However, Congress and the American people should understand that these programs—which are under judicial, executive, and legislative oversight—are vital tools for law enforcement and intelligence officials in countering the ongoing threat of terrorism.

#### Cyberspace is the New Battleground

Rosenzweig, Paul. [Visiting Fellow at Heritage Foundation]. "The State of Privacy and Security - Our Antique Privacy Rules," The Heritage Foundation. August 1, 2012,<http://www.heritage.org/research/testimony/2012/08/the-state-of-privacy-and-security-our-> antique-privacy-rules

Cyberspace is the natural battleground for enhanced analytical tools that are enabled by the technology of data collection. If our goal is to combat terrorists or insurgents (or even other nations) then the cyber domain offers us the capacity not just to steal secret information through espionage, but to take observable public behavior and information and use cyber tools to develop a more nuanced and robust understanding of their tactics and intentions. Likewise, it can be used by our opponents to uncover our own secrets. Traditionally, the concept of “surveillance” has been taken to mean an act of physical surveillance—e.g., following someone around or planting a secret camera in an apartment. As technology improved, our spy agencies and law enforcement institutions increasingly came to rely on even more sophisticated technical means of surveillance,[5] and so we came to develop the capacity to electronically intercept telecommunications and examine email while in transit.[6] To these more “traditional” forms of surveillance we must now add another: the collection and analysis of personal data and information about an individual or organization. Call the phenomenon “dataveillance” if you wish, but it is an inevitable product of our increasing reliance on the Internet and global communications systems. One leaves an electronic trail almost everywhere you go. Increasingly, in a networked world technological changes have made personal information pervasively available. As the available storehouse of data has grown, so have governmental and commercial efforts to use this personal data for their own purposes. Commercial enterprises target ads and solicit new customers. Governments use the data to, for example, identify and target previously unknown terror suspects—to find so-called clean skins who are not in any intelligence database. This capability for enhanced data analysis has already proven its utility and holds great promise for the future of commercial activity and counter-terrorism efforts.

#### Surveillance is the ONLY and BEST Defense against terror attacks

Thiessen, Marc. [Member of the White House senior staff under President George W. Bush]. "Big Brother isn’t watching you," American Enterprise Institute. June 10, 2013, <http://aei.org/article/foreign-and-defense-policy/terrorism/big-brother-isnt-watching-you/>

If the critics don’t think the NSA should be collecting this information, perhaps they would like to explain just how they would have us stop new terrorist attacks. Terrorists don’t have armies or navies we can track with satellites. There are only three ways we can get information to prevent terrorist attacks: The first is interrogation — getting the terrorists to tell us their plans. But thanks to Barack Obama, we don’t do that anymore. The second is penetration, either by infiltrating agents into al-Qaeda or by recruiting operatives from within the enemy’s ranks. This is incredibly hard — and it got much harder, thanks to the leak exposing a double agent, recruited in London by British intelligence, who had penetrated al-Qaeda in the Arabian Peninsula and helped us break up a new underwear bomb plot in Yemen — forcing the extraction of the agent. That leaves signals intelligence — monitoring the enemy’s phone calls and Internet communications — as our principal source of intelligence to stop terrorist plots. Now the same critics who demanded Obama end CIA interrogations are outraged that he is using signals intelligence to track the terrorists.

Well, without interrogations or signals intelligence, how exactly is he supposed to protect the country? Unfortunately, some on the right are joining the cacophony of condemnation from the New York Times and MSNBC. The programs exposed in these leaks did not begin on Barack Obama’s watch. When Obama continues a Bush-era counterterrorism policy, it is not an outrage

— it is a victory.

## AT NSA Abuses Power

#### The NSA has instituted Internal Checks to Prevent Privacy Loss

Rosenzweig, Paul. [Visiting Fellow at Heritage Foundation]. "The State of Privacy and Security - Our Antique Privacy Rules," The Heritage Foundation. August 1, 2012,<http://www.heritage.org/research/testimony/2012/08/the-state-of-privacy-and-security-our-> antique-privacy-rules

First, we are changing from a top-down process of command and control rule to one in which the principal means of privacy protection is through institutional oversight. To that end, the Department of Homeland Security was created with a statutorily required Privacy Officer (and another Officer for Civil Rights and Civil Liberties).[46] The more recent Intelligence Reform and Terrorism Prevention Act,[47] and the Implementing Recommendations of the 9/11 Commission Act of 2007[48] go further. For the first time, they created a Civil Liberties Protection Officer within the intelligence community. More generally, intelligence activities are to be overseen by an independent Privacy and Civil Liberties Oversight Board.[49] Indeed, these institutions serve a novel dual function. They are, in effect, internal watchdogs for privacy concerns. In addition, they naturally serve as a focus for external complaints, requiring them to exercise some of the function of ombudsmen. In either capacity, they are a new structural invention on the American scene—at least, with respect to privacy concerns. Second, and perhaps most significantly, the very same dataveillance systems that are used to advance our counter-terrorism interests are equally well suited to assure that government officials comply with the limitations imposed on them in respect of individual privacy. Put another way, the dataveillance systems are uniquely well equipped to watch the watchers, and the first people who should lose their privacy are the officials who might wrongfully invade the privacy of others.

#### There are multiple safeguards to prevent program abuse

Boot, Max. [Senior Fellow in National Security Studies at the Council on Foreign Relations]. "Stay calm and let the NSA carry on," The LA Times. June 9, 2013,<http://articles.latimes.com/2013/jun/09/opinion/la-oe-boot-nsa-surveillance-20130609>

At first blush these intelligence-gathering activities raise the specter of Big Brother snooping on ordinary American citizens who might be cheating on their spouses or bad-mouthing the president. In fact, there are considerable safeguards built into both programs to ensure that doesn't happen. The phone-monitoring program does not allow the NSA to listen in on conversations without a court order. All that it can do is to collect information on the time, date and destination of phone calls. It should go without saying that it would be pretty useful to know if someone in the U.S. is calling a number in Pakistan or Yemen that is used by a terrorist organizer. As for the Internet-monitoring program, reportedly known as PRISM, it is apparently limited to "non-U.S. persons" who are abroad and thereby enjoy no constitutional protections.

These are hardly rogue operations. Both programs were initiated by President George W. Bush and continued by President Obama with the full knowledge and support of Congress and continuing oversight from the federal judiciary. That's why the leaders of both the House and Senate intelligence committees, Republicans and Democrats alike, have come to the defense of these activities. It's possible that, like all government programs, these could be abused — see, for example, the IRS making life tough on tea partiers. But there is no evidence of abuse so far and plenty of evidence — in the lack of successful terrorist attacks — that these programs have been effective in disrupting terrorist plots.

#### The Government is passing new Surveillance legislation on the NSA

Eileen Sullivan, [Associated Press], "House Committees Pass BIll on NSA Surveillance," ABC News, [http://abcnews.go.com/Politics/wireStory/house-committees-pass-bill-nsa-surveillance-](http://abcnews.go.com/Politics/wireStory/house-committees-pass-bill-nsa-surveillance-23643354)  [23643354,](http://abcnews.go.com/Politics/wireStory/house-committees-pass-bill-nsa-surveillance-23643354) May 8, 2014.

The House crossed a major hurdle in its efforts to rein in the National Security Agency when two oversight committees agreed this week on a proposal to end the agency's practice of collecting Americans' phone records and the bulk collection of all other records, such as credit card data. The House could vote on the bill as early as this month. It was the first sign of consensus in the bitterly divided House on the controversial NSA surveillance programs since the spying was disclosed nearly a year ago. President Barack Obama has called for similar changes but is relying on Congress to hammer out the details. Senate oversight committees have yet to agree, which would be necessary before any new law is approved. The House proposal — passed Wednesday by the Judiciary Committee and Thursday by the Intelligence Committee — would strengthen privacy safeguards for Americans' communications that are swept up by the NSA. It also would require more transparency for disclosing how often private companies cooperate with the government on records requests. Obama has not formally backed any of the proposals under consideration, but a White House spokeswoman said the bill is a "very good step."

## AT Surveillance Legality

#### NSA Surveillance has legal precedent

Roger Pilon [Vice President for legal affairs at the Cato Institute] and Richard A. Epstein [Law Professor at New York University Law School], "NSA Surveillance in Perspective," Cato Institute, June 12, 2013.

In 1979, in Smith v. Maryland, the U.S. Supreme Court addressed that balance when it held that using a pen register to track telephone numbers did not count as an invasion of privacy, even in ordinary criminal cases. That’s just what the government is doing here on a grand scale. The metadata it examines in its effort to uncover suspicious patterns enables it to learn the numbers called, the locations of the parties, and the lengths of the calls. The government does not know — as some have charged — whether you’ve called your psychiatrist, lawyer or lover. The names linked to the phone numbers are not available to the government before a court grants a warrant on proof of probable cause, just as the Fourth Amendment requires. Indeed, once that warrant is granted to examine content, the content can be used only for national security issues, not even ordinary police work.

#### The Obama Administration’s Use of Surveillance is Legal

Roger Pilon [Vice President for legal affairs at the Cato Institute] and Richard A. Epstein [Law Professor at New York University Law School], "NSA Surveillance in Perspective," Cato Institute, June 12, 2013

Legally, the president is on secure footing under the Patriot Act, which Congress passed shortly after 9/11 and has since reauthorized by large bipartisan majorities. As he stressed, the program has enjoyed the continued support of all three branches of the federal government. It has been free of political abuse since its inception. And as he rightly added, this nation has real problems if its people, at least here, can’t trust the combined actions of the executive branch and the Congress, backstopped by federal judges sworn to protect our individual liberties secured by the Bill of Rights.